HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/080,574	02/25/2002	John B. Beavers	12016-0004	8681

34350 7590 12/21/2005

GUNNISON, MCKAY & HODGSON, L.L.P.
1900 GARDEN ROAD, SUITE 220
MONTEREY, CA 93940

EXAMINER
PATEL, NIRAV B

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/080,574	**Applicant(s)** BEAVERS, JOHN B.
	Examiner Nirav Patel	**Art Unit** 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-9 and 13-21* is/are rejected.

7)☒ Claim(s) *5,10-12 and 22* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on October 20, 2005 has been entered.

2. Claims 1-22 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 6-8, 13-15, 17-20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Houston et al. (US Pub No. 2002/0019945) and in view of Blakely-Fogel et al (US Patent No. 4,864,492).

As per claim 1, Houston teaches:

providing a plurality of enterprise device outputs [***paragraph 0009 lines2-3*** **"managing a large amount of security event data collected form security devices"]**, at least a portion of the outputs having different formats, each output containing an event relating to an enterprise device; translating each output into a common format event [***paragraph 0050 lines 10-11, page 5 lines 1-3*** **"the collector 225 is gathering data form variety of different security system located throughout the network, the collector 225 preferably coverts the varied data to a uniform format" Fig. 8 and Fig. 16]**, applying one or more rules from a set of rules to the knowledge-containing common format event to generate the alert indication [*paragraph 0009 lines 5-6* **"applying the criteria** (i.e. rules) **to the collected data to produce a result** (i.e. alert)" ***paragraph 0009 lines 10-13*** **"the results form applying the criteria can be rendered in a variety of different graphical formats including, but not limited to, tables, graphs, charts and tree diagrams" Fig. 15,16,17].**

Houston doesn't expressively mention that adding *knowledge* to the common format event *using knowledge base table files* to generate a knowledge-containing common format event.

However, Blakely-Fogel teaches that adding knowledge (i.e. modifying or changing) to the common format event using knowledge base table files **[Fig. 2]** to generate a knowledge-containing common format event **[Fig. 2 "Knowledge base table", Fig. 3 "change current data"].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Blakely-Fogel into the teaching of Houston to use knowledge base table and to modify the data. The modification would be obvious because one of ordinary skill in the art would be motivated to utilize the knowledge base table. It represented in rule based information tables. It contains a table of rules of the network architecture known as expert information, so user receives the knowledge of an expert to correct the input errors **[Blakely-Fogel, *col. 2 lines 3-6,19-22*].**

As per claim 2, the rejection of claim 1 is incorporated and further Houston teaches:

the common format event (i.e. an output) contains at least a generic description of a specific event occurring as part of each device output [***paragraph 0045 lines 13-17*** **"client 115 can initialize and render the display for the scope on an output device, such as a monitor or printer. The display for the scope can comprise one or more tables, charts, graphs, tree diagrams, or other renderings for presenting data to a user** (i.e. a generic description of a specific event), **Fig. 17].**

As per claim 3, the rejection of claim 1 is incorporated and further Blakely-Fogel teaches:

comparing the common format event for each network device to a number of knowledge base table entries contained in a knowledge base table **[Fig. 3, component 34]**, wherein knowledge is added from one or more of the knowledge base table entries when a match (i.e. accept) between the translated common format event and the entry in the knowledge base table is made **[Fig. 3 component 34, 36, Fig. 2].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Blakely-Fogel into the teaching of Houston to use knowledge base table and to modify the data. The modification would be obvious because one of ordinary skill in the art would be motivated to utilize the knowledge base table. It represented in rule based information tables. It contains a table of rules of the network architecture known as expert information, so user receives the knowledge of an expert to correct the input errors **[Blakely-Fogel, *col. 2 lines 3-6,19-22*].**

As per claim 6, the rejection of claim 1 is incorporated and further Houston teaches:

the knowledge-containing common format event comprises *one or more names* selected from the group of a device alert, a generic alert, a threat severity, a benign explanation, a recommended action, a common vulnerabilities and exposure code, a conclusion, and a category code, and a corresponding value for each name (i.e. event types) **[Fig. 16 "Event Type"].**

As per claim 7, the rejection of claim 1 is incorporated and further Houston teaches:

one or more rules determine when or whether the knowledge-containing common format event is generated, and final rule-based additions content of such generated events **[*paragraph 0045 lines 6-11* "the configuration criteria (i.e. rules) for the scopes can be stored on the analyzer storage module 230 of database server 145.Typical configuration criteria include sorting security event data by destination address or event type. In step 410 the persistence module 245 retrieves the configuration criteria for the desired scope from the database server 145" Fig. 16,17,18].**

As per claim 8, the rejection of claim 7 is incorporated and further Houston teaches:

the rule requires that the each output occur a number of times over a period of time before an alert indication is generated [*paragraph 0051 lines 3-9* **"the analysis of data may be initiated by a scheduled trigger within the event manager as instep 905 or in response to an external request from a user as in step 910. An analysis of data typically occurs over a defined time period. In step 915, client 115 inputs a particular start time or the scheduled start time is sent to the analyzer module 265" Fig. 9].**

As per claim 13, the rejection of claim 1 is incorporated and further Houston teaches:

the alert indication includes at least a text message describing the event contained in the output of the enterprise device [*paragraph 0045 lines 12-17* **"in step 420, client 115 can initialize and render the display for the scope on an output device, such as a monitor or printer. The display for the scope can comprise one or more tables, charts, graphs, tree diagrams, or other renderings for presenting data to a user** (i.e. a generic description of a specific event)**", Fig. 15,17].**

As per claim 14, the rejection of claim 13 is incorporated and further Houston teaches:

a threat level is included as part of the alert indication [***paragraph 0058 lines 11-14*** **"the table 1515 typically indicates when a security event took place, the source and destination addresses of the security event, the event type and priority, and the system that detected the security event" Fig. 15].**

As per claim 15, it is a system claim corresponds to method claim 1 and is rejected for the same reason set forth in the rejection of claim 1 above. Further Houston teaches a number of various files (i.e. program/software modules) [***paragraph 0008 lines 7-9***].

As per claim 17, the rejection of claim 15 is incorporated and further claim 17 is a system claim corresponds to a method claim 6 and is rejected for the same reason set forth in the rejection of claim 6 above.

As per claim 18, the rejection of claim 15 is incorporated and further Houston teaches:

the common format event comprises a message, and a number of name and value pairs derived from the output of the enterprise device **[Fig. 16].**

As per claim 19, the rejection of claim 17 is incorporated and further Houston teaches:

the rule files govern at least the frequency of the generation of the alert indication **[*paragraph 0009 lines 5-6* "applying the criteria** (i.e. rules) **to the colleted data to produce a result** (i.e. alert)**", *paragraph 0051 lines 6-9* "an analysis of data typically occurs over a defined time period. In step 915, client 115 inputs a particular start time or the scheduled start time is sent to the analyzer module 265"].**

As per claim 20, the rejection of claim 19 is incorporated and is rejected for the same reason set forth in the rejection of claim 18 above.

As per claim 21, the rejection of claim 7 is incorporated and further Blakely-Fogel teaches:

the rule adds information (i.e. modifying or changing data) to the knowledge-containing common format event (i.e. data) **[Fig. 2 knowledge base tables 20, rules 21 and Fig. 3 component 34 and 36** (change current data)**].**

4. Claims 4, 9 and 16 are rejected under 35 USC 103 (a) for being unpatentable over Houston et al in view of Blakely-Fogel et al, and further in view of Lim (US Pub No. 2004/0250133).

As per claim 4, the rejection of claim 1 is incorporated and Houston and Blakely-Fogel don't expressively mention that the enterprise devices are selected from the group consisting of a server, a firewall, a modem, a work station, a router, a remote machine, an intrusion detection system, an identification and authentication server, network monitoring and management systems, network components, and one or more combinations thereof.

However, Lim discloses that the enterprise devices are selected from the group consisting of a server, a firewall, a modem, a work station, a router, a remote machine, an intrusion detection system etc **[Fig. 1 component 12, alert form IDS/firewall, etc].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Lim into the teaching of Houston and Blakely-Fogel to use event manager for monitoring the events generated from IDS, firewall etc. The modification would be obvious because one of ordinary skill in the art would be motivated to provide better security **protection [Lim, *paragraph 0003*].**

As per claim 9, the rejection of claim 1 is incorporated and Houston and Blakely-Fogel don't expressively mention the output is one of an unauthorized login, an unauthorized physical entry, and an attempt to bypass a firewall.

However, Lim discloses that the output (i.e. triggers) is one of an unauthorized login, an unauthorized physical entry, and an attempt to bypass a firewall [*paragraph 0034, lines 1-3, 7-20* **"the triggers are in the form of an intrusion detection system, a firewall program, antivirus software, an application software and/or operating systems logs a firewall protecting a corporate network that suffers an Internet Control Message Protocol (ICMP) flood and registers a list of violations will trigger an alarm. An intrusion detection system that detects a string of commands targeted at a corporate mail server for the purpose of exploiting administrator access will trigger an alarm"].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Lim into the teaching of Houston and Blakely-Fogel to use event manager for monitoring the triggers. The modification would be obvious because one of ordinary skill in the art would be motivated to provide better security protection **[Lim, *paragraph 0003*].**

As per claim 16, the rejection of claim 15 is incorporated and further claim 16 is a system claim corresponds to a method claim 4 and is rejected for the same reason set forth in the rejection of claim 4 above.

Allowable Subject Matter

5. Claims 5, 10, 11,12 and 22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

6. Applicant's arguments filed October 20, 2005 have been fully considered but they are not persuasive.

Applicant argues that:

The Examiner has failed to callout where Blakely-Fogel et al. teaches or suggest "adding knowledge to the common format event using knowledge base table files".

Examiner maintains that:

Houston teaches a system and method for managing security event data collected from a computing network. Further, Houston teaches the scopes that filter and analyze the security event data **[Fig. 4,5,6,7]**. The configuration criteria for the scopes can be stored on the analyzer storage module 230 of database server 145 **[paragraph 0045]** and variety of criteria supports for filtering and analyzing security event data. The analyzer module 265 converts the selected criteria to a scope definition. The scope definition describes what filtering and analysis will be performed on the security event data **[Fig. 5, paragraph 0046].** Houston doesn't expressively mention that knowledge base table files which is utilized for adding knowledge to the common format event. However, Blakely-Fogel teaches that adding knowledge (i.e. modifying or changing) to the common format event using knowledge base table files **[Fig. 2]** to generate a knowledge-containing common format event **[Fig. 2 "Knowledge base table", Fig. 3**

"change current data" step 34, 36]. Further, Blakely-Fogel teaches knowledge- based intelligence which is capable to advise, correct and update the program parameters associated with network-related architecture and activities **[col. 3 lines 1-2]**. Blakely-Fogel's invention configures the protocol of a network architecture as an expert system. The expert system utilizes the knowledge of the network architecture and offers intelligent advice to system users in the event of an invalid request and processing system connected through a network.

Applicant argues that:

"Examiner has failed to make a prima facie obviousness rejection".

Examiner maintains that:

Houston's invention in the field of managing (filtering and analyzing) the security events on a network **[paragraph 0009]**. Blakely-Fogel's invention configures the protocol of a network architecture as an expert system. The expert system utilizes the knowledge of the network architecture and offers intelligent advice to system users in the event of an invalid request and processing system connected through a network. Blakely-Fogel teaches knowledge-based intelligence, which is capable to advise, correct and update the program parameters associated with network-related architecture and activities **[col. 3 lines 1-2, abstract]**.

In response to applicant's argument, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with the applicant was concerned, in order to be relied upon as basis for rejection of the claimed invention. See *In re Ortiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). Furthermore, the examiner recognizes that obviousness can only be established by combining or modifying the teaching of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to on of ordinary skill in the art. See *In re Fine*, 837 F. 2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ 2nd 1941 (Fed. Cir 1992). In this case, the combination of Houston and Blakely-Fogel teach the claimed subject matter and the combination is sufficient. In fact, Houston and Blakely-Fogel do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

7. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Sweeney et al (US 2002/0083168) disclose a method for monitoring event generated on at least one computer system.

Curtis et al (US 6,208,720) discloses the configurable and scalable rules-based thresholding system, method and computer program product for processing event records.

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP
12/16/05

[illegible]
[illegible]Y PATENT [illegible]
[illegible]LOGY CENTER